Reverse DNS lookup

From Wikipedia, the free encyclopedia

"Reverse DNS" redirects here. For other uses, see Reverse DNS (disambiguation).

In computer networking, **reverse DNS lookup** or **reverse DNS resolution** (rDNS) is the determination of a domain name that is associated with a given IP address using the Domain Name System (DNS) of the Internet.

Computer networks use the Domain Name System to determine the IP address associated with a domain name. This process is also known as *forward* DNS resolution. *Reverse* DNS lookup is the inverse process, the resolution of an IP address to its designated domain name.

The reverse DNS database of the Internet is rooted in the *Address and Routing Parameter Area* (`arpa`) top-level domain of the Internet. IPv4 uses the `in-addr.arpa` domain and the `ip6.arpa` domain is delegated for IPv6. The process of reverse resolving an IP address uses the *pointer* DNS record type (PTR record).

Internet official documents (RFC 1033 , RFC 1912 Section 2.1) specify that *"Every Internet-reachable host should have a name"* and that such names match with a reverse pointer record.

Contents

1 IPv4 reverse resolution
1.1 Classless reverse DNS method
2 IPv6 reverse resolution
3 Multiple pointer records
4 Records other than PTR records
5 Uses
6 See also
7 References
8 External links

IPv4 reverse resolution [edit]

Reverse DNS lookups for IPv4 addresses use a *reverse IN-ADDR entry* in the special domain `in-addr.arpa`. In this domain, an IPv4 address is represented as a concatenated sequence of *four decimal numbers*, separated by dots, to which is appended the second level domain suffix `.in-addr.arpa`. The four decimal numbers are obtained by splitting the 32-bit IPv4 address into four 8-bit portions and converting each 8-bit portion into a decimal number. These decimal numbers are then concatenated in the order: least significant 8-bit portion first (leftmost), most significant 8-bit portion last (rightmost). It is important to note that *this is the reverse order to the usual dotted-decimal convention for writing IPv4 addresses* in textual form. For example, an address (A) record for `mail.example.com` points to the IP address 192.0.2.5. In pointer records of the reverse database, this IP address is stored as the domain name `5.2.0.192.in-addr.arpa` pointing back to its designated host name `mail.example.com`. This allows it to pass the Forward Confirmed reverse DNS process.

Classless reverse DNS method [edit]

Historically, Internet registries and Internet service providers allocated IP addresses in blocks of 256 (for Class C) or larger octet-based blocks for classes B and A. By definition, each block fell upon an octet boundary. The structure of the reverse DNS domain was based on this definition. However, with the introduction of Classless Inter-Domain Routing, IP addresses were allocated in much smaller blocks, and hence the original design of pointer records was impractical, since autonomy of administration of smaller blocks could not be granted. RFC 2317 devised a methodology to address this problem by using *canonical name* (CNAME) DNS records.

IPv6 reverse resolution [edit]

Reverse DNS lookups for IPv6 addresses use the special domain `ip6.arpa`. An IPv6 address appears as a name in this domain as a sequence of nibbles in reverse order, represented as hexadecimal digits as subdomains. For example, the pointer domain name corresponding to the IPv6 address `2001:db8::567:89ab` is `b.a.9.8.7.6.5.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa`.

Multiple pointer records [edit]

While most rDNS entries only have one PTR record, DNS does not restrict the number. However, having multiple PTR

records for the same IP address is generally not recommended, unless there is a specific need. For example, if a web server supports many virtual hosts, there may be one PTR record for each host and some versions of name server software will allocate this automatically. Multiple PTR records can cause problems, however, including triggering bugs in programs that only expect single PTR records.[1] In the case of a large web server, having hundreds of PTR records can cause the DNS packets to be much larger than normal, which can cause responses to be truncated if they exceed the DNS 512 byte UDP message limit.

Records other than PTR records [edit]

Record types other than PTR records may also appear in the reverse DNS tree. For example, encryption keys may be placed there for IPsec (RFC 4025), SSH (RFC 4255) and IKE (RFC 4322). DNS-Based Service Discovery (RFC 6763) uses specially-named records in the reverse DNS tree to provide hints to clients about subnet-specific service discovery domains.[2] Less standardized usages include comments placed in TXT records and LOC records to identify the geophysical location of an IP address.

Uses [edit]

The most common uses of the reverse DNS include:

- The original use of the rDNS: network troubleshooting via tools such as traceroute, ping, and the "Received:" trace header field for SMTP e-mail, web sites tracking users (especially on Internet forums), etc.
- One e-mail anti-spam technique: checking the domain names in the rDNS to see if they are likely from dialup users, dynamically assigned addresses, or other inexpensive Internet services. Owners of such IP addresses typically assign them generic rDNS names such as "1-2-3-4-dynamic-ip.example.com." Since the vast majority, but by no means all, of e-mail that originates from these computers is spam, many spam filters refuse e-mail with such rDNS names.[3][4]
- A forward-confirmed reverse DNS (FCrDNS) verification can create a form of authentication showing a valid relationship between the owner of a domain name and the owner of the server that has been given an IP address. While not very thorough, this validation is strong enough to often be used for whitelisting purposes, mainly because spammers and phishers usually can't pass verification for it when they use zombie computers to forge domains.
- System logging or monitoring tools often receive entries with the relevant devices specified only by IP addresses. To provide more human-usable data, these programs often perform a reverse lookup before writing the log, thus writing a name rather than the IP address

See also [edit]

- Forward-confirmed reverse DNS

References [edit]

1. ^ glibc bug #5790
2. ^ *RFC 6763* , IETF
3. ^ spamhaus's FAQ
4. ^ reference page from AOL

External links [edit]

- Web-based DNS lookup tools at DMOZ
- ICANN DNS Operations
- RFC 2317 documents a way to do rDNS delegation for CIDR blocks
- RFC 3596 DNS Extensions to Support IP Version 6
- RDNS policies: AOL , Comcast , Craigslist , Misk.com

Categories: Searching | Domain name system

This page was last modified on 31 March 2014 at 11:02.

Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. By using this site, you agree to the Terms of Use and Privacy Policy. Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.

Privacy policy About Wikipedia Disclaimers Contact Wikipedia Developers Mobile view